UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

One black and blue Wiko cell phone ("SUBJECT DEVICE 1"); and One black Apple iPhone cell phone with a cracked screen ("SUBJECT DEVICE 2").

Case No. 5:22-mj-00480

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C § 922(g)(1); 18 U.S.C. § 924(c); 21 U.S.C. § 841(a)(1),(b)(1)(A)	See Attached Affidavit

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Pursuant to Fed. R. Crim. P. 4.1
Applicant's signature

Krista L. Gonzalez, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 8/2/2022

Judge's signature

City and state: Riverside, CA

Hon. Shashi H. Kewalramani, U.S. Magistrate Judge
Printed name and title

AUSA: John Balla, 951-276-6246

AFFIDAVIT

I, Krista Gonzalez, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint and arrest warrant against Rafael Gerardo Jr. ("GERARDO") for violations of 21 U.S.C. §§ 841(a)(1), (b)(1)(A) (Possession of Controlled Substances with Intent to Distribute), 18 U.S.C § 922(g)(1) (Felon in Possession of Ammunition), and 18 U.S.C. § 924(c) (Possession of a Firearm in Furtherance of a Drug Trafficking Crime) on July 20, 2022, in Indio, California.

2. This affidavit is also made in support of an application for a warrant to search the following digital devices (collectively, the "SUBJECT DEVICES"), in the custody of Federal Bureau of Investigation, in Riverside, California, under evidence tag number 1B71 as described in Attachment A:

a. One black and blue Wiko cell phone ("SUBJECT DEVICE 1"); and

b. One black Apple iPhone cell phone with a cracked screen ("SUBJECT DEVICE 2").

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (Possession of Controlled Substances with Intent to Distribute), 18 U.S.C § 922(g)(1) (Felon in Possession of Firearms or Ammunition), and 18 U.S.C. § 924(c) (Possession of a Firearm in Furtherance of a Drug Trafficking Crime) (the

"Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

3. I am a Special Agent ("SA") with the Federal Bureau of Investigation ("FBI") with the Los Angeles Division, Palm Springs Resident Agency in Palm Springs, California, where my duties include the investigation of violent crimes and gangs. I have been employed as a SA with the FBI since January 2020.

4. I graduated from the FBI Academy located in Quantico, Virginia, in September 2020 and received approximately 840 hours of instruction in the fundamentals of law, ethics, behavioral science, interviewing, report writing, firearms, surveillance, defensive tactics and case management. During my tenure as an FBI SA, I have participated in a variety of investigations including drug possession and trafficking, felon in possession of firearms and/or ammunition, violent crimes, bank robberies, bank fraud, wire fraud, and crimes against children.

5. As a SA, I have received training in the identification, collection, and preservation of evidence, photography, latent print collection, and crime scene investigations. I have also completed many hours of criminal investigations, including compiling information, interviewing victims, witnesses, and subjects, and collecting evidence to support the filing of criminal complaints and search warrants. During the course of my investigations, I have interviewed witnesses, conducted surveillance, participated in execution of arrest and search warrants, and reviewed various forms of evidence including telephone call detail records, bank records, invoices, photographs, recorded telephone calls, and other miscellaneous financial documents.

III. STATEMENT OF PROBABLE CAUSE

6. During the course of this investigation, I reviewed Coachella Valley Violent Crime Gang Task Force ("GTF") Police Report GE22-201-0002, body-worn camera footage from GTF Deputy Julia Camarena, spoken with officers involved in this investigation, and learned the following:

a. On Wednesday July 20, 2022, Deputy Camarena conducted a traffic stop of a 2006 Chevrolet Colorado truck at the intersection of Kenner Avenue and Jackson Street in Indio, California, for expired registration in violation of California Vehicle Code 4000(a)(1) and front window tint in violation of California Vehicle Code 26708. The driver and sole occupant of the vehicle was identified as GERARDO. Deputy Camarena asked

GERARDO if he was on probation or parole, and GERARDO revealed he was on parole.

b. After telling Deputy Camarena he was on parole, GERARDO became visually nervous. Deputy Camarena asked GERARDO to exit the vehicle while officers detained him and conducted a parole search of his person and vehicle. Deputy Camarena asked GERARDO if he had anything illegal on his person, and GERARDO revealed he had drugs on his person.

c. The parole search of GERARDO's person yielded one plastic bag in his front left pocket containing a large quantity of white crystalline substance (suspected methamphetamine[1]) and several round blue pills imprinted with "M" and "30" (suspected fentanyl[2]).

---

[1] On July 21, 2022, I weighed the substance inside of the clear plastic bag, which yielded approximately 112.45g. The substance was sent to the Drug Enforcement Agency ("DEA") laboratory on July 21, 2022. As of the signing of this affidavit, I have not received the official examination results, but the substance appears consistent, in my training and experience, with methamphetamine. Additionally, in my training and experience, that amount of methamphetamine is more than a person would typically possess for personal use.

[2] On July 21, 2022, I weighed the pills inside of the clear plastic bag, which yielded approximately 14.45g. Deputy Christian Coddington counted 97 pills inside of the bag. The pills were sent to the DEA laboratory on July 21, 2022. As of the signing of this affidavit, I have not received the official examination results, but they appear consistent, in my training and experience, with counterfeit oxycodone pills that are nearly always laced with fentanyl. Again, in my training and experience, that is more fentanyl than a person would typically possess for personal use.

d. The parole search of GERARDO's vehicle yielded one Polymer 80[3] loaded[4] Glock 34 style firearm with a ported gold barrel. The firearm was located inside of a black zipped up bag near the stick shift of the vehicle.

e. During the parole search of GERARDO's vehicle, Deputy Christian Coddington located SUBJECT DEVICE 2 in a black case in the driver's side door panel and SUBJECT DEVICE 1 on the passenger side floorboard. GERARDO told Deputy Coddington the phones were both his and that he had recently acquired "the shitty Obama phone." GERARDO did not specify which phone he was referring to. Later in the day, GERARDO told Deputy Coddington the passwords to both phones were "8-5-5-5-5-5."

f. After being read his Miranda rights, GERARDO told Deputy Camarena the substances inside of the plastic bag were methamphetamine and "blues."[5] GERARDO stated had purchased approximately two ounces of methamphetamine on July 20, 2022 for $450. GERARDO buys blue M-30 pills in quantities of 100 from the same person he buys methamphetamine from. GERARDO also claimed that the firearm located in his vehicle was not his and he was with another person while at his other residence located in Thermal the night prior and that the person left the firearm

---

[3] Polymer 80 is a manufacturer of parts kits containing firearm parts including unfinished receivers used for making privately made firearms, also known as ghost guns, which are firearms that lack a commercially applied serial number.

[4] A total of 22 rounds of live ammunition were recovered from the magazine inserted in the firearm loaded in the firearm and a separate magazine inside of the black zippered bag.

[5] Based on my training and experience, I know "blues" is slang commonly used to describe a blue M-30 pill.

inside the vehicle.[6] GERARDO would not disclose the name of this person but did reveal it is the same person from whom he buys his methamphetamine and M-30 pills. GERARDO was then placed under arrest.

12. On July 22, 2022, FBI SA Esteban Banuelos, an agent who has special training in determining the origin of firearms and ammunition, conducted an interstate nexus determination on the ammunition seized on July 20, 2022, from GERARDO. SA Banuelos determined the ammunition was not manufactured in the State of California.

7. On July 26, 2022, FBI SA Aaryn Dorsett reviewed the certified conviction records provided by the Superior Court of the State of California, County of Riverside, and verified GERARDO had been convicted of the following felony offenses punishable by a term of imprisonment exceeding one year[7]:

a. On or about July 9, 2001, in case number INF037241, in the Superior Court of the State of California, County of Riverside, for a violation of California Vehicle Code ("VC") Section 10851(a), vehicle theft, and VC 2800.1, evading a peace officer; and

---

[6] Notwithstanding his claim, in my training and experience, drug traffickers often carry firearms for protection in connection with their drug-trafficking activities.

[7] It was also discovered that GERARDO had been convicted of a felony offense from the County of San Bernardino and seven other felony offenses from the County of Riverside. I ordered a copy of the certified conviction records on July 21, 2022. As of the signing of this affidavit, I have not received the additional copies of the certified conviction records.

b. On or about June 26, 2006, in case number INF054665, in the Superior Court of the State of California, County of Riverside, for a violation of California Penal Code Section 666.5(a), vehicle theft with prior conviction.

10. My review of the records from these cases and his rap sheet indicates that, in some of his past cases, he received sentences of greater than one year in custody.

IV. TRAINING AND EXPERIENCE ON DRUG OFFENSES

6. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where the drug trafficker has ready access to them, such as on their cell phones and other digital devices.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-

mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

e. Individuals engaged in the illegal purchase or sale of firearms and other contraband often use multiple digital devices.

V. TRAINING AND EXPERIENCE ON FIREARMS OFFENSES

7. From my training, personal experience, and the collective experiences related to me by other law enforcement officers who conduct who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in

places that are readily accessible, and under their physical control, such in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with each other regarding firearms that the sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these

photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

d. Individuals engaged in the illegal purchase or sale of firearms and other contraband often use multiple digital devices.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

8. As used herein, the term "digital device" includes the SUBJECT DEVICES.

9. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has

been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

e. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

11. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

VII. CONCLUSION

13. For all of the reasons described above, there is probable cause to believe that GERARDO has committed violations of 21 U.S.C. §§ 841(a)(1), (b)(1)(A) (Possession of Controlled Substances with Intent to Distribute), 18 U.S.C § 922(g)(1) (Felon in Possession of Ammunition), and 18 U.S.C. § 924(c) (Possession of a Firearm in Furtherance of a Drug Trafficking Crime). There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES described in Attachment A.

Attested to by the applicant, FBI SA Krista L. Gonzalez
in accordance with the requirements of Fed. R. Crim. P. 4.1
by telephone on this the 2nd day of August, 2022.

UNITED STATES MAGISTRATE JUDGE

Attested to by the applicant,
FBI SA Krista L. Gonzalez,
in accordance with the requirements of
Fed. R. Crim. P. 4.1 by telephone on this
____ day of _____, 2022.

_____
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital devices (the "SUBJECT DEVICES"), seized on July 20, 2022, and currently maintained in the custody of Federal Bureau of Investigation in Riverside, California, under evidence tag number 1B71:

1. One black and blue Wiko cell phone ("SUBJECT DEVICE 1"); and

2. One black Apple iPhone cell phone with a cracked screen ("SUBJECT DEVICE 2").

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (Possession of Controlled Substances with Intent to Distribute), 18 U.S.C § 922(g)(1) (Felon in Possession of Firearms or Ammunition), and 18 U.S.C. § 924(c) (Possession of a Firearm in Furtherance of a Drug Trafficking Crime) (the "Subject Offenses"), namely:

a. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violations;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violations;

d. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs, guns, or ammunition were bought, sold, or otherwise distributed;

e. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs, guns, or ammunition;

f. Contents of any calendar or date book;

g. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations from January 20, 2022, to July 20, 2022; and

h. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

i. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created,

modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURE FOR THE SUBJECT DEVICES

3. In searching the SUBJECT DEVICES (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE(S) as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device(s) beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine

whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICES, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.